CTS handmatige configuratie met SGT-propagatie mislukt op Catalyst 9500X Layer 2-stammen

Inhoud

uitgifte

Bij het inschakelen van CTS Manual configuration met SGT propagation op Layer 2 trunk interfaces tussen Catalyst C9300L access switches en Catalyst C9500X-60L4D core switches, gaat de connectiviteit binnen enkele seconden verloren, ook al blijft een tweede uplink actief en onaangeroerd. De switch voor toegang wordt onbereikbaar vanaf beheerstations en als u de CTS-geconfigureerde uplink uitschakelt, wordt de verbinding onmiddellijk hersteld.

Specifieke symptomen die zijn waargenomen zijn:

- Access switch stopt met het ontvangen van BPDU's op getroffen VLAN's nadat CTS-handleiding met propagate sgt is ingeschakeld
- Access switch declareert zichzelf als STP-root op beide uplinks en vormt een Layer 2-lus
- Hoog aantal onbekende protocoldruppels op de access switch-interface (~1,3M druppels)
- De CTS-autorisatie is succesvol met peer SGT 9999 geïnstalleerd en geen CTS-, MKA- of MACsec-fouten
- IP-beheer van de C9300-switch wordt onbereikbaar vanaf centrale beheerstations
- Probleem treedt specifiek op wanneer verkeer met een CMD-tag het Layer 2-pad met de C9500X doorkruist

milieu

- Catalyst C9500X-60L4D core switches met Cisco IOS

- Catalyst C9300L-switches met verschillende Cisco IOS-versies (17.12.4, 17.15.4, 17.15.5)
- Layer 2 trunk uplinks met Spanning tree topologie
- CTS Handmatige configuratie met statische SGT 9999 en propageren SGT-enabled
- Dual-homed access switches aangesloten op twee core switches
- Management VLAN 50-configuratie

resolutie

Dit probleem wordt veroorzaakt door een hardwarebeperking die specifiek is voor de Catalyst 9500X- en Catalyst 9600X-platforms. De resolutie omvat het begrijpen van de platformbeperking en het implementeren van geschikte ontwerpalternatieven.

Bevestiging van platformbeperking

Engineering heeft bevestigd dat het Catalyst 9500X-platform een gedocumenteerde hardwarebeperking heeft waarbij het de Cisco MetaData (CMD)-header voor overbrugd Layer 2-verkeer niet toevoegt of verwijdert. Dit betekent:

- Verkeer dat aankomt met CMD vertrekt met CMD
- Verkeer zonder CMD vertrekt zonder CMD
- Het platform ondersteunt SGT inline tagging alleen voor gerouteerd (Layer 3) verkeer

Directionele testresultaten

Validatietests bevestigden het richtingsgedrag.

Test 1 - CTS-handleiding zonder voortplanting aan beide zijden

```
interface
 cts manual
  policy static sgt 9999
  no propagate sgt
Result: PASS - Connection remains stable
```

Test 2A - Propagatie alleen ingeschakeld op C9500X

```
! C9500X Core:
interface
 cts manual
  policy static sgt 9999 trusted
  propagate sgt

! C9300L Access:
interface
 cts manual
  policy static sgt 9999 trusted
  no propagate sgt
Result: PASS - Connection remains stable
```

Test 2B: propagatie alleen ingeschakeld op C9300L

```
! C9300L Access:
interface
 cts manual
  policy static sgt 9999 trusted
  propagate sgt

! C9500X Core:
interface
 cts manual
  policy static sgt 9999 trusted
  no propagate sgt
Result: FAIL - Connection breaks after a few seconds
```

Aanbevolen ontwerpalternatief

Aangezien de CTS-handleiding met SGT-propagatie niet betrouwbaar werkt op Layer 2-trunks

voor het C9500X-platform, is de aanbevolen oplossing om uplinks te migreren naar Layer 3-interfaces met SGT-inline tagging.

C9500X-configuratie:

```
interface <interface-id>
 no switchport
 ip address <ip-address> <subnet-mask>
 mtu 9216
 cts role-based enforcement
 cts role-based sgt-map <subnet> sgt 9999
```

C9300L-configuratie:

```
interface <interface-id>
 no switchport
 ip address <ip-address> <subnet-mask>
 mtu 9216
 cts role-based enforcement
 cts role-based sgt-map <subnet> sgt 9999
```

Oorzaak

Het probleem wordt veroorzaakt door een hardwarebeperking die specifiek is voor op Silicon One gebaseerde Catalyst 9500X- en Catalyst 9600X-platforms. Deze platforms bieden geen ondersteuning voor het verwijderen van de Cisco MetaData (CMD)-header voor overbrugd Layer 2-verkeer. Wanneer de C9300L Layer 2-verkeer met CMD-headers verzendt via SGT-propagatie, kan de C9500X-hardware de CMD-header niet verwijderen voordat pakketten worden doorgestuurd naar niet-TrustSec-eindpunten, waardoor connectiviteitsproblemen ontstaan.

Deze beperking is gedocumenteerd in de Cisco Catalyst 9500 SGT Inline Tagging Configuration Guide en is een bedoeld hardwaregedrag in plaats van een softwaredefect. De beperking stelt: "Ongeacht de handmatige cts-configuratie op de egress-interface, voegt het apparaat de Cisco MetaData (CMD)-header voor Layer 2-verkeer niet toe of verwijdert deze niet."

Andere Catalyst 9000-platforms, waaronder de Catalyst 9550-reeks, hebben deze beperking niet omdat ze verschillende hardwarearchitecturen gebruiken.

Gerelateerde inhoud

- Cisco Catalyst 9500 SGT Inline Tagging Configuration Guide
- Cisco bug ID CSCwo92798
- Cisco Technical Support en downloads

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.